NOTE: The system administrator must edit the `/var/nameserver` DNS template files manually for proper name server configuration.

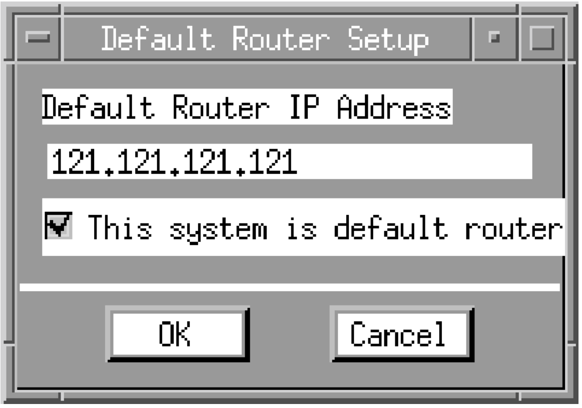
NOTE: On the Solaris 2.5.1 Operating System, a new `/etc/nsswitch.conf` file with the appropriate reference to DNS will be installed. The only change to this file is that the DNS references are added. On the HP-UX 10.20 Operating System, a new `/etc/resolv.conf` file will be installed that includes the DNS name server list and the domain search list.

Enter the IP address of the DNS server in the `DNS Server IP Search Order` field. If your workstation is acting as the primary DNS server, click on the `This system is primary DNS server` toggle. Then click on the `Add` button in the upper half of the window. You can also enter the IP address of a backup DNS server in the `DNS Server IP Search Order` field and then click on the `Add` button in the upper half of the window.

You also must add one or more domain suffixes in the `Domain Suffix Search Order` field and click on the `Add` button in the bottom half of the window. A domain suffix is a list of suffixes appended to a system name that are used to help locate the system. Click on the `OK` button when finished. The DNS domain name must match the DNS domain for the name server.

6.4.4.2 Set Routes Option

The `Set Routes` option allows the system administrator to configure a workstation with the appropriate default routing configuration. Select this option to open the `Default Router Setup` window (Figure 29). If your workstation is acting as the default router, enter the IP address of the default router in the `Default Router IP Address` field and click on the `This system is default router` toggle. If your workstation is not acting as the default router, enter the IP address of your workstation in the `Default Router IP Address` field. Do NOT click on the `This system is default router` toggle. Click on the `OK` button when finished.



Default Router IP Address

121.121.121.121

☑ This system is default router

Figure 29. Default Router Setup Window

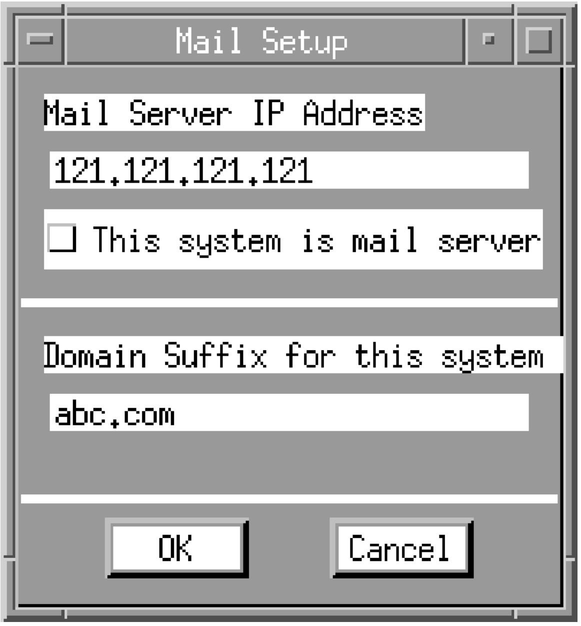
NOTE: The default router only needs to be configured for access to networks other than the LAN. The default router may also be configured during kernel installation.

6.4.4.3 Set Mail Option

NOTE: The `Set Mail` option is not available on HP workstations.

The `Set Mail` option allows the system administrator to configure mail on a workstation as either a client or a server. Select the `Set Mail` option to open the `Mail Setup` window (Figure 30). This option creates the `/etc/lib/sendmail.cf` file, which is a configuration file used for sending mail. Clicking on the `OK` button adds an entry into the operating system-specific mount configuration table.

If your workstation is acting as the mail server, enter your workstation's IP address in the `Mail Server IP Address` field and click on the `This system is mail server` toggle. If your workstation is not acting as the mail server, enter the mail server IP address in the `Mail Server IP Address` field. Do NOT click on the `This system is mail server` toggle. Click on the `OK` button when finished.



Mail Server IP Address

121.121.121.121

□ This system is mail server

Domain Suffix for this system

abc.com

Figure 30. Mail Setup Window

6.4.4.4 Set NIS Option

Network Information Service (NIS) allows user accounts to be shared across all workstations on the same domain. The `Set NIS` option is used to initialize a machine as a NIS server, add client workstations to the NIS domain, and disable NIS. The `Set NIS` option is a cascading menu that has three options: `Initialize NIS`, `Add NIS Client`, and `Remove NIS`.

Before NIS can be initialized, DNS should be configured on the master server and on the client machine. Refer to Section 6.4.4.1, *Set DNS Option*, for information on configuring DNS. In addition, an entry must be added to export the global users directory before NIS can be initialized. In other words, the NIS master workstation must have `anon=0` to allow `root` access. Then the NIS client must mount `/h/USERS/global` using the `Disk Manager` option from the `Hardware` pull-down menu to mount it, as described in the next subsection.

To initialize NIS, you need to know the NIS domain name and the NIS server host name. To initialize NIS+, you must also know the client host name and client IP address, the NIS server host name, and the network password (also known as the Secure-RPC password). Your system administrator should provide you with this information.

Adding an Entry To Export the Global Users Directory

Follow the steps below to add an entry to export the global users directory.

STEP 1: **Open the `Disk Manager` window**. Select the `Disk Manager` option from the `Hardware` pull-down menu. The `Disk Manager` window appears (Figure 8).

STEP 2: **Select `EXPORTFS`**. Click on a file system in the list to highlight it and then click on the `EXPORTFS` button. The `Export/Unexport File Systems` window appears (Figure 12).

STEP 3: **Enter the appropriate options**. Type `anon=0` in the `options` field to export the global users directory.

STEP 4: **Enter the appropriate pathname**. Type `/h/USERS/global` in the pathname field.

STEP 5: **Export the file system**. Click on the `Export` button to export the file system.

STEP 6: **Export the file system permanently**. (Solaris only) Click on the `Yes` button when the following prompt appears:

```
Do you want to permanently
export the file system?
```

STEP 7: **Confirm that the file was exported**. Click on the `EXPORTFS` button in the `Disk Manager` window and then click on the `Current` button in the `Export/Unexport File Systems` window. The `/h/USERS/global` directory should appear in the list of exported file systems.

NOTE: Refer to Subsection 6.2.3, *Disk Manager Option*, for more information on mounting and exporting file systems.

Initializing NIS on the Master or the Client

Follow the steps below to initialize NIS on the master or the client machine.

> **NOTE**: On an HP workstation, C2 must be disabled before initializing NIS. This can be done by disabling the auditing monitor daemon from the `/etc/rc.config.d/auditing` file. To do this, change `AUDITING=1` to `AUDITING=0`. Then run `/etc/tsconvert -r`.
>
> **NOTE**: It is recommended that the master server be initialized before any client machines are initialized.

STEP 1: **Initialize NIS**. Select the `Initialize NIS` option from the `Set NIS` cascading menu option.

STEP 2: **Enter the NIS domain name**. An `ENTER A RESPONSE` window appears. Enter the domain name at the prompt and click on the `OK` button or press [`RETURN`]. This is the name of the domain that will include the master and client machines.

> **NOTE**: The NIS domain name must contain two parts separated by a `.` (period).

STEP 3: **Set the machine as the master server or as a client**. The `RESPOND TO THE QUESTION` window appears with the following prompt: `Is this machine the Master NIS Server?` If the machine is the client, click on the `No` button and proceed to STEP 4; if the machine is the server, click on the `Yes` button and proceed to STEP 11.

STEP 4: **Enter the NIS server host name**. The `ENTER A RESPONSE` window appears with the following prompt: `Enter the NIS Server Host Name`. Enter the name of the machine designated as the server at the prompt and click on the `OK` button or press [`RETURN`].

STEP 5: **Acknowledge that the NIS server host is reachable**. An `INFORMATIONAL MESSAGE` window appears with the following message: `[NIS Server Host Name] is reachable`. Click on the `OK` button or press [`RETURN`]. If you are on an HP, proceed to STEP 11.

STEP 6: **Continue the initialization**. (Solaris only) The following message appears:

```
Initializing client [client name] for domain [domain name]
Once initialization is done, you will need to reboot your
machine. Do you want to continue?
```

Type `Y` and press [`RETURN`] to continue, or type `N` and press [`RETURN`] to exit the script. If you type `Y`, proceed to STEP 7; if you type `N`, proceed to STEP 11.

STEP 7: **Enter the network password**. (Solaris only) Several messages appear, ending with the following:

```
At the prompt below, type the network password (also known as
the Secure-RPC password) that you obtained either from your
administrator or from running the nispopulate scripts.
Please enter the Secure-RPC password for root:
```

Enter a password as described in the NOTE that follows STEP 8 and press [RETURN].

STEP 8: **Enter the login password for `root`**. (Solaris only) Enter a password at the prompt and press [RETURN]. The following message appears: `Your network has been changed to your login one. Your network and login passwords are now the same.` Proceed to STEP 9.

NOTE: (Solaris only) This password remains in the password file even if NIS is removed from the client machine. The following message will appear if NIS has already been configured and if the password has already been entered.

```
If the machine was initialized before as a NIS+ client, please enter the
root login password as the network password. Or re-type the network
password that your administrator gave you.
```

Enter the appropriate password and press [RETURN]. The following message appears:

```
Your network has been changed to your login one. Your network and login
passwords are now the same.
```

STEP 9: **Enter and confirm a secman password**. (Solaris only) The `ENTER A PASSWORD` window appears after several minutes. Enter a secman password and press [RETURN]. Re-enter the password to verify it and press [RETURN]. Then click on the `OK` button.

STEP 10: **Enter and confirm a sysadmin password**. (Solaris only) The `ENTER A PASSWORD` window appears after several minutes. Enter a sysadmin password and press [RETURN]. Re-enter the password to verify it and press [RETURN]. Then click on the `OK` button.

STEP 11: **Wait for a message indicating that you need to reboot the machine**. While a NIS client is initializing, do *not* reboot until a reboot message appears. If you are initializing a NIS client on an HP machine, a few minutes may pass before this message appears. If you are initializing a NIS master on an HP machine, a message appears telling you that NIS is initializing.

STEP 12: **Acknowledge that the machine needs to be rebooted**. An `INFORMATIONAL MESSAGE` window appears with the following message: `Please Reboot this machine`. Click on the `OK` button to close the window.

STEP 13: **Reboot the machine**. Select the `Reboot System` option from the `Hardware` pull-down menu. The `Reboot` dialog box appears with the following prompt: `Do you want to shutdown and reboot the computer?`Click on the `OK` button to reboot the machine.

NOTE: The system takes several minutes to reboot. During this time, several informational messages appear, including the following:

```
NIS domainname is [domain name]
```

The domain name will be the name you specified in STEP 2. This message confirms that NIS has been initialized on the machine.

NOTE: The following message also appears on the master server *only* upon this initial reboot:

```
The password used will be nisplus
Use this password when the nisclient script requests the network
password.
```

This is the password to be entered in STEP 7 when NIS is initialized on the client machine.

When the reboot is complete, the `DII COE Login` window appears. NIS is configured.

Adding a NIS+ Client

Follow the steps below to add a machine as a NIS+ client. This section applies to Solaris only.

NOTE: NIS+ clients can only be added on the master server machine.

NOTE: When adding a NIS client, the server and client must recognize each other through inclusion in the local hosts table.

STEP 1: **Select the `Add NIS Client` option**. Select the `Add NIS client` option from the `Set NIS` cascading menu option on the NIS server.

STEP 2: **Enter the client host name**. The `ENTER A RESPONSE` window appears. Enter the client host name at the prompt and click on the `OK` button.

STEP 3: **Enter the client IP address**. The `ENTER A RESPONSE` window appears. Enter the IP address at the prompt and click on the `OK` button.

STEP 4: **Enter and confirm the client `root` password**. The `ENTER A PASSWORD` window appears. Enter the `root` password and press [`RETURN`]. Re-enter the password to verify it and press [`RETURN`]. Then click on the `OK` button.

STEP 5: **Determine if you want to initialize the machine as a client**. The following prompt appears:

```
Initializing client [name] for domain “.”. Once initialization
is done, you will need to reboot your machine. Do you wish to
continue?
```

Type `Y` or `N` and press [`RETURN`].

STEP 6: **Reboot the machine**. Reboot the machine if you added a NIS+ client. Select the `Reboot System` option from the `Hardware` pull-down menu. The `Reboot` dialog box appears with the following prompt: `Do you want to shutdown and reboot the computer?` Click on the `OK` button to reboot the machine.

NOTE: No message appears to tell you if the process was successful.

Removing NIS

The `Remove NIS` option disables NIS from the system, which removes the domain name and, upon reboot, does not start NIS processes. Follow the steps below to disable and remove NIS.

STEP 1: **Select the `Remove NIS` option**. Select the `Remove NIS` option from the `Set NIS` cascading menu option.

STEP 2: **Disable and remove NIS**. The `RESPOND TO THE QUESTION` window appears with the following message: `Do you wish to disable and remove NIS?`Click on the `No` button to close the window, or click on the `Yes` button to disable and remove NIS.

NOTE: No message appears to tell you if the process was successful.

STEP 3: **Acknowledge that the machine needs to be rebooted**. (HP only) An informational message appears prompting you to reboot the machine. Click on the `OK` button.

STEP 4: **Reboot the machine**. Select the `Reboot System` option from the `Hardware` pull-down menu. The `Reboot` dialog box appears with the following prompt: `Do you want to shutdown and reboot the computer?`Click on the `OK` button to reboot the machine.

NOTE: The system takes several minutes to reboot. During this time, several informational messages appear, including the following:

```
NIS domainname is
```

This domain name field will be blank if NIS was removed successfully.

The system reboots to the DII COE Login screen.

NOTE: If you want to re-enable NIS, reboot the workstation first, then initialize NIS.

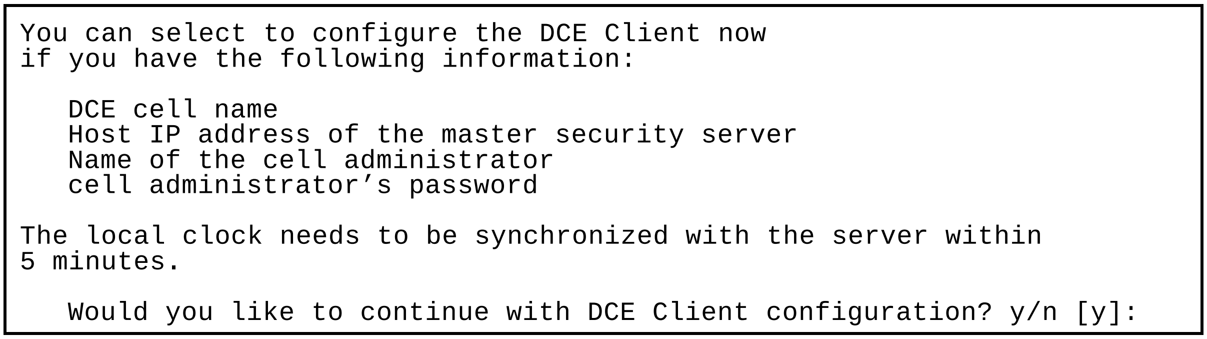
6.4.5 DCE Option

The `DCE` option is a cascading menu that has four options: `Configure DCE Client`, `Configure DTS server`, `Configure Audit server`, and `Unconfigure DCE`. These options are described in the following subsections.

NOTE: The `DCE` option appears on Solaris only.

6.4.5.1 Configure DCE Client Option

The `Configure DCE Client` option allows the system administrator to configure a workstation as a client system in a DCE cell. Select the `Configure DCE Client` option to open the `DCE Client Configuration` screen (Figure 31).



```
You can select to configure the DCE Client now
if you have the following information:

   DCE cell name
   Host IP address of the master security server
   Name of the cell administrator
   cell administrator’s password

The local clock needs to be synchronized with the server within
5 minutes.

   Would you like to continue with DCE Client configuration? y/n [y]:
```

Figure 31. DCE Client Configuration Screen

DCE is normally configured during initial system installation; however, DCE configuration can be skipped during the system installation process. Refer to the *DII COE Kernel Installation Guide (Solaris 2.5.1)* for information about configuring the DCE client during initial system installation.

The `Configure DCE Client` option allows DCE client configuration to be performed after the initial installation. The interface is through a series of prompted questions and responses from a terminal window.

NOTE: The local clock *MUST* be synchronized to within 5 minutes of the server clock for the system to configure DCE. If the times are not synchronized, DCE configuration will fail.

NOTE: You must unconfigure DCE before attempting to configure DCE.

NOTE: Do not continue with the client configuration if a server is not configured and operating.

NOTE: If the system is configured into a cell, you must reconfigure the system before starting the DCE client configuration.

Follow the steps below to configure a workstation as a client system in a DCE cell.

STEP 1: **Determine if you would like to continue with the DCE client configuration**. Type `Y` or `N` at the prompt and press [RETURN].

STEP 2: **Enter the cell name**. Enter the cell name at the prompt and press [RETURN].

STEP 3: **Enter the Internet Protocol (IP) address of the master security server**. Enter the IP address at the prompt and press [RETURN].

STEP 4: **Enter the name of the cell administrator**. Enter the name of the cell administrator at the prompt and press [RETURN].

STEP 5: **Enter the cell administrator's password**. Enter the password at the prompt and press [RETURN].

STEP 6: **Determine if you would like to configure this node as a DFS client server**. Type `Y` or `N` at the prompt and press [RETURN]. If you are on an HP workstation, proceed to STEP 7; if you are on a Sun workstation, proceed to STEP 11.

STEP 7: **Determine where the cache is located**. The following prompt appears: `Is the cache: 1. in memory 2. on the local drive.`Type `1` or `2` and press [RETURN].

STEP 8: **Enter the size of the cache**. The following prompt appears: `Enter size of cache (10000)`. Enter a new cache size or press [RETURN] to accept the default value.

STEP 9: **Determine the cache directory**. The following prompt appears: `Enter the name of the cache directory (/opt/dcelocal/var/adm/dfs/cache)`. Enter a directory name or press [RETURN] to accept the default directory.

STEP 10: **Determine if the DFS client is to be configured as an NFS gateway**. The following prompt appears: `Would you like to configure this DFS client as an NFS gateway?` Type `N` and press [RETURN].

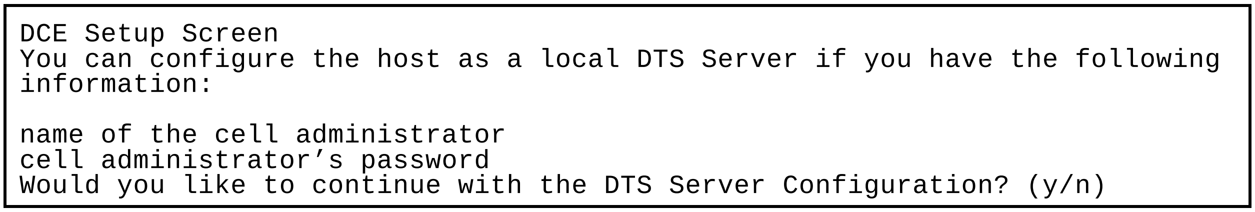
STEP 11: **Determine if you would like to configure this node as a local DTS server**. Type `Y` or `N` at the prompt and press [RETURN].

STEP 12: **Determine if you would like to configure this node as an audit server**. Type `Y` or `N` at the prompt and press [RETURN].

STEP 13: **Exit the DCE client configuration display**. Type `q` at the prompt and press [RETURN] to exit the DCE client configuration display.

6.4.5.2 Configure DTS Server Option

The `Configure DTS server` option allows the system administrator to configure the host as a local DTS server. Select the `Configure DTS server` option to open the `DCE Server Configuration` screen (Figure 32).



```
DCE Setup Screen
You can configure the host as a local DTS Server if you have the following
information:

name of the cell administrator
cell administrator’s password
Would you like to continue with the DTS Server Configuration? (y/n)
```

Figure 32. DCE Server Configuration Screen

Follow the steps below to configure the host as a local DTS server.

STEP 1: **Determine if you want to continue with the DTS server configuration**. Type `Y` or `N` and press [RETURN].

STEP 2: **Enter the name of the cell administrator**. Enter the name at the prompt and press [RETURN].

STEP 3: **Confirm the name of the cell administrator**. Enter the name again and press [RETURN].

STEP 4: **Enter the cell administrator’s password**. Enter the password at the prompt and press [RETURN].

STEP 5: **Exit the DTS server configuration display**. Type `q` at the prompt and press [RETURN] to exit the DTS server configuration display.

6.4.5.3 Configure Audit Server Option

Follow the steps below to configure the host as an audit server.

STEP 1: **Select the `Configure Audit` server option**. Select the `Configure Audit` server option from the `DCE` option cascading menu.

STEP 2: **Determine if you want to continue with the audit server configuration**. Type `Y` or `N` at the prompt and press [RETURN].

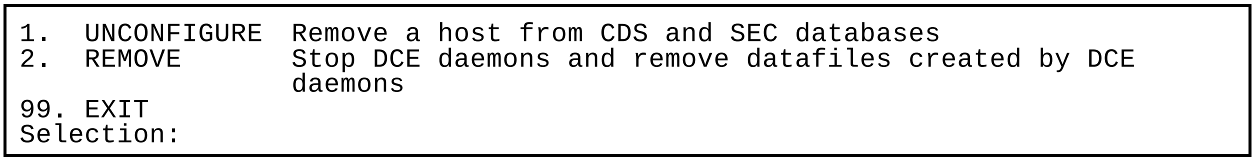
STEP 3: **Exit the audit server configuration display**. Type `q` at the prompt and press [RETURN] to exit the audit server configuration display.

6.4.5.4 Unconfigure DCE Option

The `Unconfigure DCE Client` option allows the system administrator to remove the system as a client from a DCE cell. The interface is through a series of prompted questions and responses from a terminal emulator window.

> **NOTE**: Do not continue with the client configuration if a server is not configured and operating.

Select the `Unconfigure DCE Client` option to open the `DCE Setup` window (Figure 33).



```
1.  UNCONFIGURE  Remove a host from CDS and SEC databases
2.  REMOVE       Stop DCE daemons and remove datafiles created by DCE
                 daemons
99. EXIT
Selection:
```

Figure 33. DCE Setup Window

Follow the steps below to unconfigure the DCE client.

STEP 1: **Choose to unconfigure the DCE client**. Type `1` at the prompt and press [RETURN].

STEP 2: **Enter the cell administrator's account name**. Enter the cell administrator’s account name at the prompt and press [RETURN].

STEP 3: **Enter the password of the cell administrator**. Enter the password at the prompt and press [RETURN].

STEP 4: **Determine if you want to force unconfiguration**. Type `Y` or `N` at the prompt and press [RETURN].

STEP 5: **Exit the DCE client configuration display**. Type `q` at the prompt and press [RETURN] to exit the DCE client configuration display.

6.5 Removing Global Data

The `COERemoveGlobal` command line tool is a security management tool that allows the system administrator to remove global segment data on the global users/profile workstation. Global segment data should be removed only if all segments referring this profile first have been deinstalled. The specified segment must be available currently on the local workstation. When removing an Account Group segment, the whole directory will be removed (e.g., `h/USERS/global/Profiles/SampleAcctGrp`). Reference the *DII COE Security Manager's Guide (HP-UX 10.20 and Solaris 2.5.1)* for more information on security management capabilities.

Follow the steps below to use the `COERemoveGlobal` command line tool.

STEP 1: **Log in as `sysadmin`**. Type `sysadmin` at the `Name` prompt and press [RETURN].

STEP 2: **Enter the `sysadmin` password**. Type the `sysadmin` password at the `Password` prompt and press [RETURN]. The System Administration software appears.

STEP 3: **Open a terminal emulator window**.

> **NOTE**: Command line tasks are performed in terminal emulator windows. Follow the steps below to access a terminal emulator window.
>
> STEP 1: Double-click on the Application Manager control on the CDE Front Panel to open the `Application Manager` window.
>
> STEP 2: Double-click on the `DII_APPS` folder in the `Application Manager` window to open the `Application Manager - DII_APPS` folder.
>
> STEP 3: Double-click on the `SA_Default` folder to open the `Application Manager - SA_Default` window. This window contains both a `DTterm` icon and an `XTerm` icon.
>
> STEP 4: Double-click on either the `DTterm` icon or the `XTerm` icon to open the window.

STEP 4: **Log in**. Log in as `sysadmin` at the terminal emulator login prompt and press [RETURN].

STEP 5: **Enter the appropriate password**. Enter the `sysadmin` password at the password prompt and press [RETURN].

STEP 6: **Remove global data for the specified segment**. Type the following at the prompt:

```
COERemoveGlobal [flags] segment[RETURN]
```

NOTE: If you need help, type `COERemoveGlobal` without any parameters. The following message appears:

```
Usage: COERemoveGlobal [flags] segment
The usable flags are:
-h, H, ?:   Display the help message
-V:         Display the tool’s version number
-p <path>   Use Path to Establish path for subsequent file names.

This tool will remove global data for the specified segment

NOTE: If no Path is specified, /h will be used.
```

STEP 7: **Determine if global data has been deleted for the specified segment**. If the command was successful, the following message appears:

```
Successful Removal of Global Data for Segment [segment name]
```

If the command was not successful, the following message appears:

```
Unsuccessful Removal of Global Data for Segment [segment name]
```

The prompt then reappears.

6.6 Changing Workstation Security Levels

The `COESecLevel` command line tool is a security management tool that allows the system administrator to change the security level of a workstation. Reference the *DII COE Security Manager’s Guide (HP-UX 10.20 and Solaris 2.5.1)* for more information on security management capabilities. Follow the steps below to use `COESecLevel`.

STEP 1: **Log in as `sysadmin`**. Type `sysadmin` at the `Name` prompt and press [RETURN].

STEP 2: **Enter the `sysadmin` password**. Type the `sysadmin` password at the `Password` prompt and press [RETURN]. The System Administration software appears.

STEP 3: **Open a terminal emulator window**.

NOTE: Command line tasks are performed in terminal emulator windows. Follow the steps below to access a terminal emulator window.

STEP 1: Double-click on the Application Manager control on the CDE Front Panel to open the `Application Manager` window.

STEP 2: Double-click on the `DII_APPS` folder in the `Application Manager` window to open the `Application Manager - DII_APPS`folder.

STEP 3: Double-click on the `SA_Default` folder to open the `Application Manager - SA_Default` window. This folder contains both a `DTterm` icon and an `XTerm` icon.

STEP 4: Double-click on either the `DTterm` icon or the `XTerm` icon to open the window.

STEP 4: **Log in as `sysadmin`**. Log in as `sysadmin` at the terminal emulator login prompt and press [RETURN].

STEP 5: **Enter the `sysadmin` password**. Enter the `sysadmin` password at the password prompt and press [RETURN].

STEP 6: **Change the security level of the workstation**. Type the following at the prompt:

```
COESecLevel [security level][RETURN]
```

NOTE: If you would like a list of the security levels or need help, type `COESecLevel` without any parameters. The following message appears:

```
Usage:
             COESecLevel Security Level>
where <security level> is UNCLASS, CONFIDENTIAL, SECRET,
TS, SCI.
```

(`TS` stands for top secret; `SCI` stands for sensitive compartmented information.)

STEP 7: **Close the terminal emulator window**. Type the following command at the prompt:

```
logout [RETURN]
```

STEP 8: **Reboot the system**. Select the `Reboot System` option from the `Hardware` pull-down menu. The `Reboot` dialog box appears with the following prompt: `Do you want to shutdown and reboot the computer?`Click on the `OK` button to reboot the machine.

STEP 9: **Log in as sysadmin or secman**. Log in as sysadmin or secman at the terminal emulator login prompt and press [RETURN].

STEP 10: **Enter the appropriate password**. Enter the sysadmin or secman password at the password prompt and press [RETURN]. The security banner will have changed to show the new security level.

6.7 Auditing

Auditing is a security management capability that allows the system administrator to enable or disable auditing. Reference the *DII COE Security Manager's Guide (HP-UX 10.20 and Solaris 2.5.1)* for more information on security management capabilities.

6.7.1 Auditing on Solaris 2.5.1

Enabling Auditing

Auditing on Solaris can be started automatically after initial kernel installation by typing `Y` at the following prompt: `This script is used to enable the Basic Security Module (BSM). Shall we continue with the conversion now (y/n)?` Refer to the *DII COE Kernel Installation Guide (Solaris 2.5.1)* for information on starting auditing automatically after initial kernel installation.

If auditing on Solaris was not started after initial kernel installation or has been disabled, auditing can be enabled by logging in as `root` and executing the shell script `/etc/security/bsmconv`, which configures the Basic Security Module.

NOTE: Auditing can only be enabled or disabled by the `root` user.

After the `bsmconv` command has been run, the system must be rebooted to initialize the auditing subsystem.

Disabling Auditing

Auditing is disabled by logging in as `root` and executing the shell script `/etc/security/bsmunconv`. The system must be rebooted after this script is executed.

6.7.2 Auditing on HP-UX 10.20

Enabling or Disabling Auditing From SAM

NOTE: Refer to vendor documentation for more information on using SAM.

Follow the steps below to start or stop audit from SAM.

STEP 1: **Log in as sysadmin**. Type sysadmin at the Name prompt and press [RETURN].

STEP 2: **Enter the `sysadmin` password**. Type the `sysadmin` password at the `Password` prompt and press [RETURN]. The System Administration software appears.

STEP 3: **Access the Application Manager**. Double-click on the Application Manager control on the CDE Front Panel to open the `Application Manager` window. Reference Section 5, *Common Desktop Environment*, for more information about CDE.

STEP 4: **Open the `DII_APPS` folder**. Double-click on the `DII_APPS` folder in the `Application Manager` window to open the `Application Manager - DII_APPS` folder.

STEP 5: **Open the `SA_Default` folder**. Double-click on the `SA_Default` folder to open the `Application Manager - SA_Default` window.

STEP 6: **Execute the `sam` application**. Double-click on the `sam` icon.

STEP 7: **Select the `Auditing and Security` icon**. The `System Administration Manager` window appears. Double-click on the `Auditing and Security` icon.

STEP 8: **Select either the `Audited Users` icon, `Audited Events` icon, or the `Audited System Calls` icon**. The `SAM Areas:Auditing and Security` subwindow appears. Double-click on the `Audited Users` icon, the `Audited Events` icon, or the `Audited System Calls` icon.

STEP 9: **Convert to a trusted system**. Click on the `Yes` button to convert to a trusted system if the following message appears. If the message does not appear, proceed to STEP 12.

```
          You need to convert to a Trusted System before
          proceeding.
The conversion process does the following things:

1.  It saves a copy of "/etc/passwd" in the file
    "/etc/passwd.old.sav".
2.  It then moves the passwords from "/etc/passwd" into a new
    "hidden" password database (the file
    "/.secure/etc/passwd").
3.  It invalidates all passwords in "/etc/passwd" by replacing
    them with "*".  For more details, refer to the "HP-UX
    System Security" manual.

          Do you wish to convert to a Trusted System now?
```

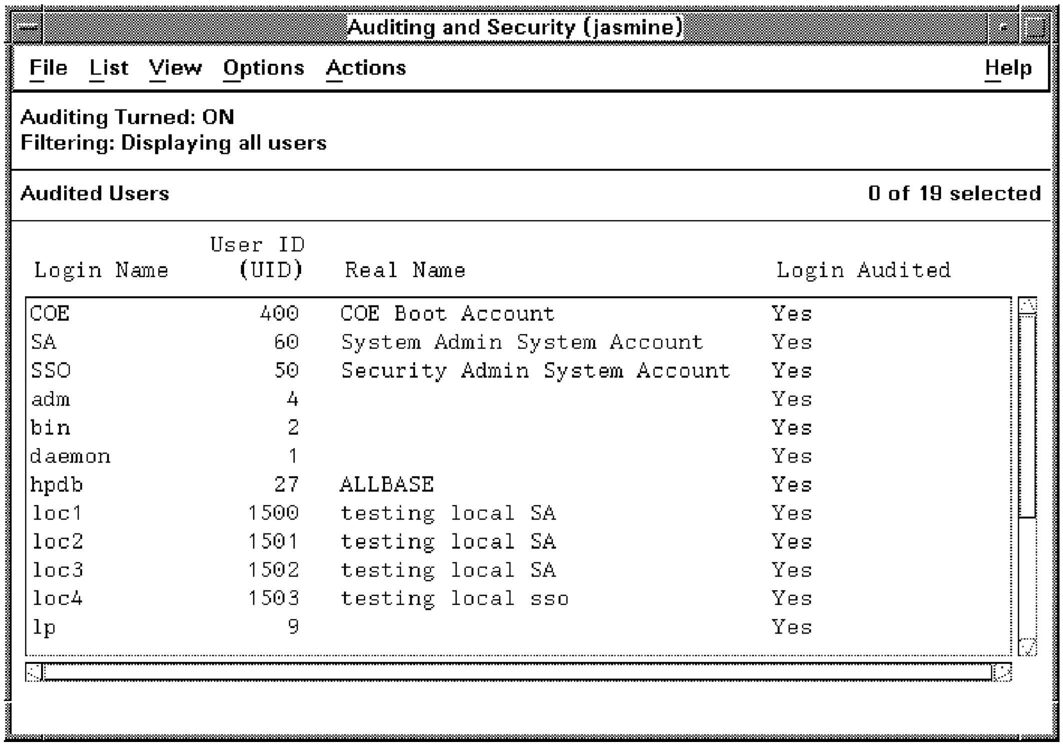
STEP 10: **Affirm that you want to convert to a trusted system**. Click on the `Yes` button if the following message appears:

```
WARNING:   The change to a Trusted System is irreversible!
           Are you sure you want to continue?
```

STEP 11: **Finish with the conversion**. Click on the `OK` button if the following message appears:

```
Converting to a trusted system ...
Task succeeded.  Press OK to continue.
```

STEP 12: **Turn auditing on or off.** The `Auditing and Security` window appears (Figure 34). Click on an entry in the window to highlight it and select either the `Turn Auditing Off` or `Turn Auditing On` option from the `Actions` pull-down menu to stop or start audit, respectively.



Auditing Turned: ON
Filtering: Displaying all users

Audited Users 0 of 19 selected

Login Name	User ID (UID)	Real Name	Login Audited
COE	400	COE Boot Account	Yes
SA	60	System Admin System Account	Yes
SSO	50	Security Admin System Account	Yes
adm	4		Yes
bin	2		Yes
daemon	1		Yes
hpdb	27	ALLBASE	Yes
loc1	1500	testing local SA	Yes
loc2	1501	testing local SA	Yes
loc3	1502	testing local SA	Yes
loc4	1503	testing local sso	Yes
lp	9		Yes

Figure 34. Auditing and Security Window

Using Shadow Password Files

To use a shadow password file on HP, type `/etc/tsconvert`. This utility updates the shadow password file and removes all password information from the default password file. Once this program has completed, the machine must be rebooted.

To discontinue use of a shadow password file on HP, type `/etc/tsconvert -r`. This utility restores the default password file with the actual encrypted password information. Once this program has completed, the machine must be rebooted.

6.8 Changing the sysadmin Password

Follow the steps below to change the `sysadmin` password.

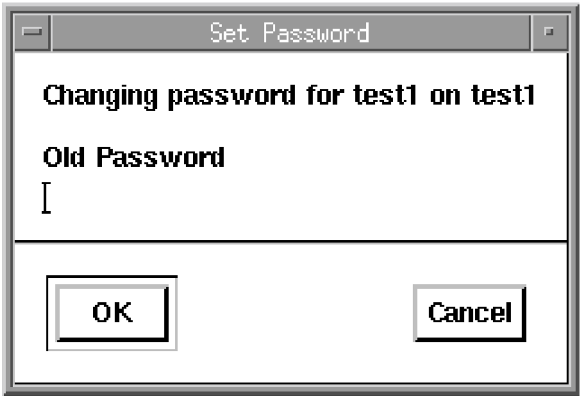
STEP 1: **Log in as `sysadmin`**. Type `sysadmin` at the `Name` prompt and press [RETURN].

STEP 2: **Enter the `sysadmin` password**. Type the `sysadmin` password at the `Password` prompt and press [RETURN]. The System Administration software appears.

STEP 3: **Access the Application Manager**. Double-click on the Application Manager control on the CDE Front Panel to open the `Application Manager` window.

STEP 4: **Select the `DII_TOOLS` folder**. Double-click on the `DII_TOOLS` folder in the `Application Manager` window to open the `Application Manager - DII_TOOLS` folder.

STEP 5: **Select the `Chg Password` icon**. Double-click on the `Chg Password` icon to open the `Set Password` window (Figure 35).



Changing password for test1 on test1

Old Password

Figure 35. Set Password Window

STEP 6: **Enter the current `sysadmin` password**. Enter the current `sysadmin` password in the Old Password field and click on the `OK` button.

STEP 7: **Enter the new `sysadmin` password**. The `New Password` window appears. Enter the new `sysadmin` password in the `Enter New Password` field and click on the `OK` button.

STEP 8: **Verify the new `sysadmin` password**. The `Verify New Password` window appears. Enter the new `sysadmin` password in the field and click on the `OK` button.

STEP 9: **Acknowledge that the `sysadmin` password has changed**. Click on the `OK` button when the following message appears:

```
Your password has been successfully updated!
```

7. Error Recovery Guidelines

> **NOTE**: Never power off the system without first executing a shutdown. Doing so could cause irreparable damage. If the system has already been brought down incorrectly, refer to Subsection 8.4, *Repairing File Systems*.

The following topics are covered:

- Recovering from basic errors
- Troubleshooting multiple monitors
- Identifying hardware problems
- Repairing file systems
- Reporting problems.

7.1 Recovering From Basic Errors

Access to all System Administration menus and options is required to perform error recovery procedures.

> **IMPORTANT**! The following procedures are listed according to "risk factor"—that is, from the least to the greatest risk of damaging files or losing data. Always begin corrective action with the procedure that poses the least risk.

If these steps do not correct the problem, contact the number listed in Section 8.5, *Reporting Problems*.

Options are unavailable:

- Access to options may be restricted for the user's account. Check with the security manager.

Window hangs or menu option has been disabled:

- Select the `Close All` option from the `SA System` pull-down menu (on the System Administration menu bar). All windows launched from the menu bar or from the `DII_APPS` folder will close. Windows launched from the CDE front panel will not close.

Reboot the system:

STEP 1: Notify users on remote monitors that their applications will soon terminate.

STEP 2: Select the `Reboot System` option from the `Hardware` menu on the System Administration menu bar.

STEP 3: Restart the system with user login.

Power up/power down the system with pointer and keyboard operational:

C See Chapter 3, *Operating Guidelines*.

Power up/power down the system with pointer frozen:

STEP 1: Turn off the monitor and peripherals.

STEP 2: Turn off the CPU.

STEP 3: Wait approximately 30 seconds.

STEP 4: Turn on the monitor and peripherals.

STEP 5: Turn on the CPU.

STEP 6: Restart the system with the user login.

Reinstall the DII COE:

STEP 1: Use the original installation tapes if a network installation is not possible.

STEP 2: Follow the instructions to reinstall the DII COE.

7.2 Troubleshooting Multiple Monitors and Keyboards

Monitor or keyboard fails to respond:

C A reboot may solve the problem.

C Rebooting the computer in a multiple monitor environment means all monitors will go down. When working with multiple monitors, contact all users before rebooting.

Monitor is black:

C Make sure the monitor cable is connected properly.

C Make sure the monitor is connected to a power supply and is turned on.

C The video switch may have incorrect input or output, or may be turned off.

Monitor is black with small yellow squares (HP only):

C Make sure each monitor is connected to the correct port on the back of the CPU.

Second monitor in a dual-eye configuration is gray:

C Make sure keyboards are connected correctly. This monitor is the second eye of a dual-eye configuration.

Trackball does not respond:

C Reboot the machine. If this does not work, try using a different trackball. If the trackball still does not respond, there may be a wiring problem in the cable.

Keyboard does not respond:

C Make sure the keyboard is connected properly.

C The keyboard may be connected properly but the monitor may not "echo" the typed characters to the screen. Rebooting the machine usually solves this problem.

7.3 Identifying Hardware Problems

When the workstation is turned on, the CPU runs a hardware check. If the hardware check is successful, the following occurs:

C The system boots from the default boot device.

C The system displays configuration information, followed by the login prompt.

C Observe the boot information for system/hardware problems. If the boot fails, a disk problem has occurred. Refer to the hardware manual for more information.

7.4 Repairing File Systems

If the system was brought down unexpectedly (e.g., power failure, turned off without proper shutdown), it is designed to repair the file system when powered up.

C The system should never be powered down while the file system is being repaired. To do so would cause further damage to the file system.

C If power is fluctuating, leave the system off until power is re-established.

7.5 Reporting Problems

To receive immediate assistance with a problem or to report a problem, call the DII COE hotline at (703) 735-8682 between the hours of 9:00 a.m. to 5:00 p.m. Eastern Standard Time. The hotline is located at the Operational Support Facility (OSF) in Sterling, Virginia.

If a problem cannot be corrected by the procedures described in this document, follow these guidelines to report it:

STEP 1: **Make sure the problem can be repeated**.

STEP 2: **Record pertinent information**. Record the problem, the last steps leading to the problem, and the frequency with which the problem occurs.

STEP 3: **Describe attempts to solve the problem**.

Appendix A - CSE-SS Functionality

A.1 CSEXDM

A.1.1 Overview

The X Display Manager (XDM) segment provides users with the capability to log in to a DII COE workstation via a graphical user interface (GUI). The `/h/COE/Comp/CSEXDM/bin/xdm` executable is a modified version of the X11 Release 4, X Display Manager and is initiated as part of the workstation's boot sequence.

A.1.2 CSEXDM Configuration

Resources affecting XDM functionality and various GUI characteristics initially have predefined default values. These resource values can be altered from the default settings by modifying various configuration files. Access with `root` privileges to a terminal emulator window and a text editor is required to perform these modifications.

The following is the main configuration file used by CSEXDM:

```
/h/COE/Comp-/CSEXDM/data/config/xdm-config
```

This file contains XDM resources in the X resource format. These resources control the behavior of CSEXDM.

It should be noted that because CSEXDM can manage more than one display connection (e.g., X-terminals connected to the host machine), some of the resources apply to a single display device (per-display resources), while others apply to the CSEXDM process in general (global resources). For per-display resources, values are assigned using the following syntax, where `#` is the display number:

```
DisplayManager._#.resource:   value
```

To assign a per-display resource value to all displays, an asterisk is used as a wild card in place of the `_#` (e.g., `DisplayManager*resource: value`). For global resource values, a simple dot notation is used (e.g., `DisplayManager.resource: value`).

Table 1 explains the resources set within the `xdm-config` file and shows their default settings.

Table 1. xdm-config File Resource Settings

Resource	Default Setting	Description
terminateServer	true	Specifies if the X server should be terminated when a session terminates instead of resetting it.
systemPath	/usr/bin:/usr/sbin/usr /openwin/bin:/etc (etal.)	Specifies the default value for the PATH environment variable for root users.
userPath	/usr/bin:/bin:/usr/sbin:/usr /local/bin (etal.)	Specifies the default value for the PATH environment variable for normal users.
authorize	false	Controls if CSEXDM generates and uses authorization for the server connections.
resources	/h/COE/Comp/data /app-defaults/xdm-resources	File defining the CSEXDM authentication widget's resources. These resources control the appearance of the CSEXDM opening login window.
startup	/h/COE/Comp/CSEXDM/data/etc /Xstartup	File containing commands executed by CSEXDM when the windowing session is started.
session	/h/COE/Comp/CSEXDM/data/etc /Xsession	File containing commands executed by CSEXDM when the windowing session is initialized.
reset	/h/COE/Comp/CSEXDM/data/etc /Xreset	File containing commands executed by CSEXDM when the windowing session is terminated.
serverEnv	/h/COE/Comp/CSEXDM/data /config/xdm-env	File containing extra environment variable assignments required by CSEXDM.
screensaverTimeout	5	Specifies the number of minutes before an inactive login screen is blanked.
rootLogins	false	Specifies if logins are allowed by root users (users having an ID of 0).
servers	/h/COE/Comp/CSEXDM/data /config/xdm-servers	File that contains an entry for each of the displays that should be managed by CSEXDM.
errorLogFile	/h/COE/Comp/CSEXDM/data/log /xdm-errors	File where CSEXDM errors are written. This file will also contain any errors generated by the Xstartup, Xsession, and Xreset files.
consoleLogFile	/h/COE/Comp/CSEXDM/data/log /xdm-console	File where console messages are written.
pidFile	/h/COE/Comp/CSEXDM/data/log /xdm-pid	File where the process identification of the CSEXDM process is stored.
dbmFile	/h/COE/Comp/CSEXDM/data/etc /xdmlogin	Directory and base filename for the database file that record the number of log in failures for each user.
maxInvalidLogins	3	Maximum number of log in failures before the user is locked out of the workstation.
loginResetTimeout	1440	Number of minutes before a workstation with invalid login attempts is reset to zero log in attempts (24 hours).

Table 1. xdm-config File Resource Settings

Resource	Default Setting	Description
`lockoutMailRecipient`	`secman`	Specifies the user or mail alias to receive mail messages when users are locked out of a workstation.
`lockoutMailSubject`	`User Locked Out`	Specifies the subject line for mail messages sent when users are locked out of a workstation.
`dceAuthenticate`	`false`	Specifies if DCE user authentication is performed.
`dceLogin`	`/usr/bin/dce_login`	Specifies the default path for invoking the DCE login script.
`useDisplayConsole`	`true`	Specifies if the Console Window will be displayed when CSEXDM is executed.

NOTE: After resource modification, the workstation must be rebooted for the changes to take effect.

A.1.3 Environment Variables

Alter the environment variables in the `/h/COE/Comp/CSEXDM/data/config/xdm-env`file as appropriate for the site.

A.1.4 CDE Invocation

CSEXDM is preconfigured to invoke the CDE desktop upon a successful login. By default, it determines if CDE has been installed by testing for the existence of `/usr/dt/bin/Xsession`(see `/h/COE/Comp/CSEXDM/data/etc/Xsession`). If that file exists, it assumes CDE is properly configured and starts up the CDE `Xsession` script. If `/usr/dt/bin/Xsession`is not found, it assumes CDE has not been installed and defaults to invoking the MWM window manager as the user session. In this case the mwm binary should exist in one of the path components specified by the `DisplayManager*userPath`resource in the `xdm-config` file.

A.1.5 Unlocking a Locked Out User

To unlock users previously locked out due to too many invalid login attempts, invoke the CSEXDM_User_Account_Informationbinary. This binary opens a window that displays a variety of user login information, such as whether the user is currently logged in, the user's full name, and the user's home directory. Users who have an uppercase L next to their name are locked out users. To unlock a user in this condition, highlight the user name then choose clear_failures from the File menu. Repeat this process for all locked out users who should be unlocked.

The CSEXDM_User_Account_Informationbinary also can be used to unlock locked users on remote hosts. To view user information on a remote workstation, an entry in the remote systems /.rhosts must exist for the local system. For example, if CSEXDM_User_Account_Information is being run from workstation A the following entry must exist in workstation B's /.rhosts file:

```
A     root
```

For more information, view the User_Account_Information.1manual page located in /h/COE/Comp/CSEXDM/man.

On platforms where the CSEXDM_User_Account_Informationbinary is not available, the CSEXDM_clear_failuresbinary can be used to unlock locked users. Execute the following command as the root user from the shell prompt in a terminal emulator window, where uname is the user name of the locked out user:

```
CSEXDM_clear_failures uname
```

Refer to the clear_failures.1manual page for more information.

A.1.6 DCE

The segment can be configured to perform DCE user authentication against the local cells Security Registry and to download the user security credentials. To enable this feature, first make sure the system has been properly configured to be a DCE client; this should be tested by invoking /usr/bin/dce_login with a valid user name and password. Second, set the DisplayManager*dceAuthenticateresource to true in the /h/COE/Comp/CSEXDM/data/config/xdm-configfile. Finally, reboot the workstation. CSEXDM_xdm should attempt to perform a DCE authentication in addition to the local UNIX authentication.

If the DCE authentication fails and the user is a valid UNIX user, the user is still permitted access to the system; however, the user will not have any DCE security credentials for his or her login session.

A.1.7 Servers

In the file /h/COE/Comp/CSEXDM/data/config/xdm-config if the value of the DisplayManager.servers resource is set to /h/COE/Comp/CSEXDM/data/config/xdm-servers, then modify the xdm-servers file according to the xdm.1 manual page. The xdm.1 manual page is located in /h/COE/Comp/CSEXDM/man.

A.1.8 Manual Pages

The xdm.1, User_Account_Information.1, and clear_failures.1 files in the /h/COE/Comp/CSEXDM/man/ subdirectory are the on-line manual pages for the CSEXDM_xdm, CSEXDM_User_Account_Information, and CSEXDM_clear_failures applications.

A.2 CSECON

A.2.1 Overview

The CSECON segment provides a console window (read-only window) that remains open for the life of the user's login session and cannot be closed, although it may be iconified.

The console window, /h/COE/Comp/CSECON/bin/CSECON_xdcons, is started by CSEXDM and displays error and notification messages written to standard error and /dev/console during the login session. Errors generated by CSECON_xdcons are stored in the /h/COE/Comp/CSEXDM/data/log/xdcons-errors file. The Close function on the CSECON window is disabled by specifying the following resource in the following /usr/lib/X11/app-defaults/Mwm resource file:

```
   Mwm*xdcons*clientFunctions: -close
```

All xdcons resources are specified in the /h/COE/Comp/CSEXDM/xdcons-resources file and described in the Table 2.

Table 2. CSECON Resources

Resource	Default Setting	Description
foreground	old lace	Defines the color of text displayed in the console window.
background	darkslategrey	Defines the background color of the console window.
iconic	true	Defines the initial iconified state of the console window.
geometry	+0+0	Defines the location of the console window on the screen. These coordinates resolve to the upper left corner of the screen.
text.columns	80 columns	Defines the number of columns the console will display.
text.rows	4 rows	Defines the number of rows the console window will display.
minHeight	39 pixels	Defines the minimum height to which the console window can be reduced.
minWidth	36 pixels	Defines the minimum width to which the console window can be reduced.
heightInc	13 pixels	Defines the height of the icon used to represent the console window.
widthInc	6 pixels	Defines the width of the icon used to represent the console window.
title	Console Window	Defines the title of the console window.
iconName	Console	Defines the title of the window icon.

A.2.2 Turning Off the Console Window

For some of the platforms supported by DII COE, the opening of the console window can be prevented by setting a resource value. If the resource DisplayManager*useDisplayConsole exists in the /h/COE/Comp/CSEXDM/data/config/xdm-configfile, the console window can be disabled. To disable the opening of the console window, set the default value from true to false. To enable the opening of the console window, set the value to true. Superuser privileges and a text editor are required to modify the xdm-config file. To make the change effective, the user must log out and log in again. Setting this resource value determines the console window configuration for all users local to that workstation.

A.2.3 Manual Pages

The xdcons.1 file in the /h/COE/Comp/CSECON/man/subdirectory is the on-line manual page for the CSECON_xdcons application.

A.3 CSEPAS

A.3.1 Overview

The CSEPAS segment provides users with the capability to change their own passwords and provides the security manager with the capability to assign a password to a general user. Both of these utilities use a rule-based password checking capability.

The user can change his or her own password through invocation of the `CSEPAS_userpass` executable. `CSEPAS_userpass` allows the user to enter a new password and re-enter the password for verification purposes. The `/h/data/app-defaults/CSEPAS`resource file is used for setting the font and color characteristics of the GUI windows. `CSEPAS_userpass` implements the public domain `passwd+` software, which provides its rule-based password checking capability. The `/h/COE/Comp/CSEPAS/data/passwd.data`file contains the construction rules for a valid password. The rules contained in this file are discussed in the next section.

The security manager assigns passwords to users through invocation of the `CSEPAS_Assign_Passwords`executable. `CSEPAS_Assign_Passwords`displays a selectable list of users who currently exist on the system. `CSEPAS_userpass` is invoked for each user that is selected for password assignment.

A.3.2 Changing Password Construction Parameters

To determine the parameters by which a password is constructed, the appropriate set of rules in `/h/COE/Comp/CSEPAS/data/passwd.data`must be selected. To modify the `passwd.data` file, superuser privileges are required. It is recommended that the rules themselves not be modified, with the exception of the password length rule. The desired combination of rules can be selected through the insertion or removal of commenting marks at the beginning of the rules records. A standard ASCII text editor can be used to modify the `passwd.data` file. When the `passwd.data` file is in its initial state, a default set of password rules are selected.

In the case of every rule, to prevent the use of a rule in the construction of a password, comment out the rule by inserting a `#` character at the beginning of the line where the rule is specified. Be aware that some rules are interrelated and may require all associated rules to be commented out to prevent the checking of that password construct. Uncomment the rule by deleting the `#` from the beginning of the line where the rule is specified.

In the `passwd.data` file, the password rules are found beginning on line 102. The first rule of the set disallows the user’s login name being used as his or her password. Note that to allow users to use their log in name as their password the circular shift rule, identified in a following paragraph, must also be commented out. The second rule is similar to the first rule and disallows the use of the user’s log in name typed in reverse being used as their password.

The third through the eleventh rules, discussed in the following paragraph, depend on the GECOS information having been included in the user's password record. If this information is not included with the password record, then these rules are not checked in the construction of new passwords.

The third and forth rules disallow the user's first name and reversed first name being used as their password. The fifth and sixth rules disallow the user's last name and reversed last name being used as their password. The seventh and eighth rules disallow the user's office and reversed office being used as their password. The ninth and tenth rules disallow the user's phone number and reversed phone number being used as their password. The eleventh rule disallows the user's initials being used as their password.

The twelfth and thirteenth rules disallow the newly entered password from being the same as the previous password. The last rule in this section disallows the use of the user's ID from being the password or being contained within the password.

The next rule found in the `passwd.data` file disallows use of a circular shift of the user name as a password.

The next section of the file contains five rules that govern the use of host name and domain name in the construction of passwords. The first two rules in this section disallow the host name and reversed host name of the local workstation being used as passwords. The next two rules disallow the domain name and reversed domain name being used as passwords. The last rule disallows domained host name being used as a password.

The next section of the file contains four rules that disallow words that are found in two separate dictionary files from being used as passwords. Note that both of the rules for a dictionary must be commented out to allow words found in that dictionary to be used as passwords. The two dictionary files are `/h/COE/Comp/CSEPAS/data/trivial.dict`and `/h/COE/Comp/CSEPAS/-data/full.dict`

The last rule in the file determines the required length of the password. The default length of a constructed password is eight characters. To adjust the length of the constructed password change the value of the number after the < character to the minimum desired length. The password can be adjusted to be 1 to 8 characters long. For the benefit of the user, it is suggested that if the password length limit is modified, that the length specified in the error message portion of the rule also be changed to reflect the new length. If this rule is commented out, a password from length 1 to 8 characters can be constructed.

A.3.3 Manual Pages

The `userpass.1`, `Assign_Passwords.1`, and `passwdplus.1` files in the `/h/COE/Comp-/CSEPAS/man/` subdirectory are the on-line manual pages for the `CSEPAS_userpass` and `CSEPAS_Assign_Passwords` applications.

A.4 CSELCK

A.4.1 Overview

The CSELCK (xlock) segment provides the DII COE with an automatic session locking mechanism that activates when the mouse and keyboard have been idle for a configurable amount of time.

A.4.2 Operation

The condition of a session when it is in an idle state is referred to as deadman. The CSELCK segment considers deadman to have two distinct phases. During the first phase of the deadman, `/h/COE/Comp/CSELCK/bin/CSELCK_xautolock`automatically locks the screen if the keyboard and mouse have been idle for a configurable time limit by invoking `/h/COE/Comp/CSELCK/bin/xlock` During the second phase of the deadman, xlock takes a deadman action if the keyboard and mouse remain idle for a configurable time limit after the screen has been automatically locked. The xlock resources are specified in the file `CSELCK` located in the `/h/COE/Comp/CSELCK/data/app-defaults`subdirectory. These resources are described in Table 3. Superuser privileges and a text editor, such as "vi" editor, are required to change this file. The xlock resources are located at the end of the `CSELCK` file. At the beginning of this file, after some records of modification, are the settings for the various screen saver modes which are used by the `CSELCK_xlock` screen locking application. The settings for these screen saver modes are described in the `CSELCK_xlock` manual pages.

Be aware that the CDE which comes with the DII COE kernel also contains a screen saver function. Depending on whether it is enabled and the settings of its time out value, it may engage before the CSELCK can perform its session locking function.

A.4.3 Changing Screen Lock Time Out

The `CSELCK_xautolock` process is initially invoked when xdm executes "Xsession" during user log in. This file is located in the `/h/COE/Comp/CSEXDM/data/etc/`subdirectory. This file must be edited to change the period of time that `CSELCK_xautolock` waits before locking the screen of an idle workstation. Superuser privileges and a text editor, such as "vi" editor, are required to change this file. This task is intended to be performed by the System Administrator. The `-time` option of the command line which invokes the `CSELCK_xautolock` process is the value which needs to be changed. The command line appears as follows:

```
if [ -d /h/COE/Comp/CSELCK ]; then
   /h/COE/Comp/CSELCK/bin/CSELCK_xautolock -time 5 -locker
   “/h/COE/Comp/CSELCK/bin/CSELCK_xlock -name CSELCK
   -remote -allowaccess +allowroot >&- 2>&-” &
fi
```

Note that the line is replicated here with the default options. The maximum value that the `-time` option can be is 60 minutes and the minimum value is 1 minute, the default, as shown, is 5 minutes. The workstation must be rebooted after the change is made to make it effective.

Table 3. CSELCK (Xlock) Resources

Resource	Default Setting	Description
deadmanTimeout	30 minutes	Specifies the number of minutes after the screen is locked to execute the deadman action.
deadmanAction	none	Specifies the actions to be performed when deadman timeout expires. It may consist of the string "none" or one or more of the following space separated strings: "notify", "terminate", and "script". If "none" is set, no action will be performed. If "notify" is set, the person or mail alias, specified by the deadmanMailRecipient resource, will be notified by email that the workstation has been left unattended. If "terminate" is set, the user's session, including all processes owned by the user, will be terminated. If "script" is set, the shell script named by the deadmanScript resource will be executed.
deadmanWarningTimeout	60 seconds	Specifies the number of seconds before executing the deadmanAction to display a warning message.
deadmanWarning	Depends on the setting of the deadmanAction resource	Specifies the warning message to display. If the deadmanAction contains the "terminate" flag, the deadmanWarning default is "WARNING: Inactive session will be terminated in %d seconds!". Otherwise the default is to not display a warning message.
deadmanWarningBell	on	Controls whether an audible beep is sounded at one-second intervals during the display of the warning message.
deadmanScript	No default	The script executed when the deadman timeout expires if the deadmanAction resource is set to "script". The script must reside in the `/h/CSELCK/data/etc` directory.
deadmanMailRecipient	secman	Specifies the user or mail alias used by the deadman capability when sending mail messages.
deadmanMailSubject	Deadman Timeout	Specifies the subject line of deadman mail messages.

A.4.4 Manual Pages

The `CSELCK_xautolock.1` and `CSELCK_xlock.1` files in the `/h/COE/Comp/CSELCK/man/` subdirectory are the on-line manual pages for the `CSELCK_xautolock` and the `CSELCK_xlock` applications.

Appendix B - Communications

B.1 The DII COE Network

An HP or a SPARC loaded with the DII COE can be configured as a stand-alone machine or networked in a server/client relationship.

B.1.1 Stand-alone Configuration

A stand-alone machine is its own server. It retains data without relying on a networked server. It shares data (1) through messages transmitted over configured comms ports or (2) by floppy diskette or tape.

B.1.2 Network Configuration

The communications processor holds all track and comms data. When installing software, the communications processor should be installed first, followed by its client machines. Client machines depend on the server for data, especially data from the track database. Communications processor functions include:

C Processing incoming and outgoing messages

C Decoding incoming messages

C Correlating track information

C Routing outgoing messages.

If the server goes down, the Track Database Manager (Tdbm) warning window informs the user that the server is down. Although the user can view track information, no track database actions (local or shared) are processed.

B.2 Interface Description

The DII COE supports two interface types: serial and LAN.

B.2.1 Serial Interface: RS-232, RS 422, MIL-188

A serial interface is used for serial communication between systems. If systems are at the same site, connect them directly. If systems are at different sites, connect them through a secure modem, such as a STU III.

B.2.2 LAN Interface: Ethernet and Fiber Optic Cabling

Ethernet and fiber optic cabling are used to enable communications between two or more workstations on a LAN. Each machine is assigned a unique name and IP address on the network, which are used by system files.

B.2.3 Protocols

B.2.3.1 TCP/IP

Transmission Control Protocol (TCP) moves data in a continuous, unstructured byte stream. It provides full-duplex service, acknowledgment of data received, and data flow control.

Internet Protocol (IP) provides network layer services to the TCP/IP protocol suite. IP is responsible for forwarding packets through a network based on IP addresses. IP relies on TCP to guarantee delivery of packets.

B.2.3.2 X.25

X.25 is used for a Wide Area Network (WAN) of computers connected by a Packet Switching Network (PSN), such as the Defense Data Network "DSNET1". (X.25 is generally used by ashore sites only.)

B.3 Physical Connections

B.3.1 Serial

B.3.1.1 Requirements for a Direct Connection

A 2-, 3-, and 7-pin connection is required to connect systems located in the same installation.

B.3.1.2 Requirements for STU III Connection

The STU III must support an RS-232 connection. If it does not, the user must request an RS-449-to-RS-232 adapter from the manufacturer.

An HP workstation requires a DB 9 female-to-DB 25-male cable. Certain models of STU III require voltage on pins 4 and 20, which the HP workstation does not supply. A special adapter must be used.

B.3.2 LAN

B.3.2.1 Requirements for an Ethernet Interface

C Use an AUI interface with a DB 15-pin connector between the workstation and the transceiver.

C The copper LAN interface may have a BNC connection between transceivers.

C The network must be terminated at both ends. Use a terminating 50W resistor on each end.

C If the workstation is a stand-alone configuration, the LAN connections on the workstation must be terminated. Use a 50W resistor on each end.

B.3.2.2 Requirements for a Fiber Optic Connection

C Use an AUI interface with a DB 15-pin connector between the workstation and the transceiver.

C The transceiveres must reside at each computer connected by fiber optics. These boxes have dual-ring capability to ensure continued transmission.

For example, if a transmission is interrupted by a broken fiber optic or connection, it is automatically routed to the second ring.

B.3.3 X.25

Requirements for an X.25 Connection (HP)

C If the system is configured for DDN communications, the Serial A port must be the DDN/X.25 interface device. No other device may be configured to the TTYA port.

C A DB 15 connects the machine to a modem and encryption device with an X.25 interface.

C The X.25 card provides synchronous RS-232 (DTE) error-free transmission over the PSN.

C There may be many interfaces, such as crypto, modem, or leased line, between the computer and the actual PSN.

B.4 Communication and Broadcast Configuration

Modify fields to configure a communications channel. Keep in mind the following general information:

- C Standard comms settings should be used. Changing some settings, such as baud rate, parity, or stop bits, may cause data to be garbled. For example, if messages are garbled, it is likely that the transmitting and receiving sites do not have the same values set for the baud rate and related fields.
- C XON/XOFF should never be used for baudot data connections. Toggle on the `XON/XOFF` checkbox to enable the use of software flow control to stop and resume transmission.
- C If the `RTS/CTS` checkbox is toggled on, hardware flow control is enabled.
- C Make sure the comms interface configuration matches the flow control settings.

B.4.1 Starting Comms Channels

A comms channel must be turned on before it can be used.

Turn channels on and off one of two ways:

- C Highlight the channel and then select `START`, `STOP`, or `RESTART` from the pop-up menu.
- C Toggle the `AUTOSTART` checkbox ON in the `COMMS EDIT` window. This turns a channel on at system startup.

The `STATUS` column indicates status of each channel: `ON` or `OFF`.

Important:

- C A comms channel can only be turned on if the designated device exists. For example, a DTC comms channel is assigned to TTYC2. If a multiplexer is not connected to the TTYC port, this channel cannot be turned on, but it can be reassigned to an existing port.
- C A channel must be ON to open its status window.

Highlight the channel and select the `WINDOW` pop-up option.

B.4.2 Starting Broadcasts

A broadcast must be turned on before it can be used. Broadcasts are turned on and off using the BROADCASTS option from the FOTC/BCST menu. The BROADCASTS window displays a list of available broadcasts.

Turn broadcasts on and off one of two ways:

C Highlight the broadcast; select START from the pop-up menu.

C Toggle the AUTOSTART checkbox ON in the BROADCAST EDIT window. This turns the broadcast on at system startup.

The STATUS column indicates status of each broadcast: ON or OFF.

B.4.3 Message Transmission

Messages are sent manually (using an XMIT option) and automatically (using a broadcast).
To transmit a message, make sure the communications channel is turned on, the channel is configured properly, and the channel can transmit messages.

NOTE: Manual transmissions are not allowed on the DTC channel; only automatic transmissions are allowed via the DTC broadcast.

To broadcast a message, make sure the appropriate comms channels are running, as described in the previous section, and the appropriate broadcast programs are running, as described below.

B.4.4 Message and Broadcast Headers

To set a default message header for manual transmissions, click DEFAULT in the HEADER EDIT window pop-up menu. This header is used for all options that have a manual transmit capability, such as tracks and overlays.

Each broadcast has its own header. If DEFAULT is selected while creating a header for a broadcast, the broadcast header becomes the default message header. This header is used for manual transmissions and for the broadcast.

B.5 STU III Configuration

A serial interface comms channel must first be configured for the STU III connection (see Section B.3, *Physical Connections*). Set the device to the port connected to the STU III. Use serial interface defaults for the other settings: `data type=ASCII`, `parity=NONE`, `stop bit=1`, `baud rate=2400`, `data size=8`, `RECV` and `XMIT=ON`.

C An entry must be made in the Auto-Forward Table. (See *Auto-Forward Table* in the *Unified Build User's Guide*.)

C An entry must be made in the Sources reference table if in FOTC mode. (See *Source XREF Table* in the *Unified Build User's Guide*.)

C Both STU IIIs must be in Remote Control Mode with Secure Access Control System (SACS) enabled.

C Both STU IIIs must have proper ACLs loaded.

C STU IIIs with SACS support auto-answer auto-secure-no operators are needed. In this mode, Voice/Secure Voice options are unavailable.

SACS grants access to designated STU IIIs, as identified in the ACL on the local STU III.

Three requirements for secure authentication of automatic, incoming calls are (1) ACL header, (2) DAO code, and (3) Keyset ID.

STU IIIs (including STU III SACS) without these codes are excluded, and cannot gain access or connect with STU-IIIs that share DAO codes or keyset IDs.This creates a closed network. Unauthorized calls are disconnected before the line to JMCIS is opened. If two STU IIIs can talk to each other, but cannot transmit data, their internal modes may be different. Check baud rates: synchronous and asynchronous must match.

B.5.1 Downloading ACL

The following tables illustrate the sequence of an ACL download. This sequence has been tested on AT&T devices only.

STEP 1: Insert the Master CIK.

STEP 2: Click on the `MENU` option.

OBSERVE	PRESS
`Main Menu Secure Voice`	`NEXT`
`Main Menu Secure Data`	`NEXT`
`Main Menu Show Config`	`NEXT`
`Main Menu Change Config`	`SELECT`
`Change Config Security Config`	`SELECT`
`Security Config SACS Disable`	`NEXT`
`Security Config SACS Options`	`SELECT`
`SACS Options SACS Control`	`NEXT`
`SACS Options Auto Access Control`	`NEXT`
`SACS Options Far-end ID`	`NEXT`
`SACS Options Access List`	`SELECT`
`ACCESS LIST MENU Load ACL Via DTE`	`SELECT`
`WAITING FOR ACL start DTE transfer`	(begin download)
`RECEIVING ACL please wait`	(wait until finished)
`ACL RECEIVED nnn show new ACL`	`NEXT`
`ACL RECEIVED nnn save new ACL`	`SELECT`
`NEW ACL SAVED previous menu`	`MENU`

B.5.2 Temporarily Disabling SACS ACL

STEP 1: Insert the Master CIK.

STEP 2: Click on the `MENU` option.

OBSERVE	PRESS
`Main Menu Secure Voice`	`NEXT`
`Main Menu Secure Data`	`NEXT`
`Main Menu Show Config`	`NEXT`
`Main Menu Change Config`	`SELECT`
`Change Config Security Config`	`SELECT`
`Security Config SACS Disable`	`SELECT`
`SACS Disable on/off change Disable`	`SELECT`

B.5.3 Autodialing Between Two AT&T STU IIIs

STEP 1: Insert the Master CIK.

STEP 2: Click on the `MENU` option to turn auto-answer on.

After the ACL is downloaded, but before it is put in Remote Control Mode, auto-answer must be on.

If the display indicates one or more AASD rings, auto-answer is on.

PRESS	**PRESS**
`NEXT` until "`Change Config`"	`SELECT`
`NEXT` until "`Security Config`"	`SELECT`
`NEXT` until "`SAC Options`"	`SELECT`
`NEXT` until "`SACS Control`" (ensure SASCTRL is enabled.)	`SELECT`

PRESS	**PRESS**
`MENU`	`MENU` (again)
`NEXT` until "`Change Config`"	`SELECT`
`NEXT` until "`Security Config`"	`SELECT`
The display panel will read SACS Disable (ensure SACS Disable is `OFF`)	`SELECT`

PRESS	**BUTTON**
`MENU`	`MENU` (again)
`NEXT` until "`Change Config`"	`SELECT`
`NEXT` until "`Security Config`"	`SELECT`
`NEXT` until "`SAC Options`"	`SELECT`
`NEXT` until “`Auto Access Ctrl`”	(Ensure Auto Access Ctrl is `ON`)

PRESS	**BUTTON**
MENU	`MENU` (again)
`NEXT` until"`Change Config`"	`SELECT`
`NEXT` until "`Auto-Answer`"	`SELECT`

B.5.4 Configuring Specific STU-III Models

Motorola SECTEL 1000/2000:

- This device provides the auto-secure feature, but does not allow auto-answer, nor does it support SACS.
- The default data mode is 2400 baud, asynchronous.
- An RS-232 port is included, allowing direct connection to the system.
- A serial communications interface must be used.

RCA STU III:

- The STU III data port is an RS-232 (DB 25) or an RS-449 (DB 37) connection, depending on manufacturer and model.
- RS-232 and RS-449 share the same signal levels but have a different pinout.
- RS-449 ports must be converted to RS-232 to work with the system. These converters are included with the STU III.

Table 4 illustrates the conversion requirements of a STU III RS-449 configuration to an RS-232.

RS-449 (STU-III)	RS-232 (TDP)
1–Shield	1–Shield
4–Send Data (+)	2–TXD
6–Receive Data	3–RXD
7–Request to Send	4–RTS
9–Clear to Send	5–CTS
11–Data Mode	6–DSR
19–Common Return	7–Common
20–Receive Common	
22–Send Data (-)	
37–Send Common	
12–Terminal Ready	20–DTR

Table 4. RS-449 to RS-232 Conversion

Follow the steps below to configure an RCA STU III:

STEP 1: Press `PROGRAM`.

STEP 2: Press `SETUP`.

STEP 3: Press `YES` at "`set terminal options`."

STEP 4: Press `YES` at "`set standard options`." The standard settings are:

- Dialing mode: TONE
- Comm mode: FULL DUPLEX
- Data Ports: 2400 ASYNC
- Remote Capable: DISABLED
- A-lead Control: ENABLED
- Dual Home: Line 1 only.

Appendix C - Multiple Monitor and Keyboard Configurations

A single, properly equipped HP TAC-3 (Tactical Advanced Computer) CPU can drive any of the following configurations:

C Single-eye console with 1-3 single-eye remote monitors

C Dual-eye console with 1-2 single-eye remote monitors

C Dual-eye console with a dual-eye remote monitor.

Tables 5 and 6 illustrate the recommended single-eye and dual-eye monitor connection schemes. For potential difficulties the user may encounter in a multi-monitor environment, reference Subsection 8.2, *Troubleshooting Multiple Monitors and Keyboards*.

Single-eye Console	**Remote 1**	**Remote 2**	**Remote 3**
Monitor: crt00 Keyboard: KYBD4	None	None	None
Monitor: crt00 Keyboard: KYBD1	**Single-eye** Monitor: crt01 Keyboard: KYBD2	None	None
Monitor: crt00 Keyboard: KYBD1	**Single-eye** Monitor: crt01 Keyboard: KYBD2	**Single-eye** Monitor: crt10 Keyboard: KYBD3	None
Monitor: crt00 Keyboard: KYBD1	**Single-eye** Monitor: crt01 Keyboard: KYBD2	**Single-eye** Monitor: crt10 Keyboard: KYBD3	**Single-eye** Monitor: crt11 Keyboard: KYBD4

Table 5. Single-eye Console

Dual-eye Console	Remote 1	Remote 2
Top Monitor: crt01 Bottom Monitor: crt00 Keyboard: KYBD1	None	None
Top Monitor: crt01 Bottom Monitor: crt00 Keyboard: KYBD1	**Single-eye** Monitor: crt10 Keyboard: KYBD4	None
Top Monitor: crt01 Bottom Monitor: crt00 Keyboard: KYBD1	**Single-eye** Monitor: crt10 Keyboard: KYBD3	**Single-eye** Monitor: crt11 Keyboard: KYBD4
Top Monitor: crt01 Bottom Monitor: crt00 Keyboard: KYBD1	**Dual-eye** Top Monitor: crt11 Bottom Monitor: crt10 Keyboard: KYBD3	None

Table 6. Dual-eye Console

Appendix D - Database Size Limits

This appendix lists database limits for various DII COE files.

Tracks	Limits
Platform/Ambiguity	1500
Emitter	1500
Link	1024
Acoustic	100
Unit	500
SI	450
External	0

Table 7. Track Limits

Other Track Ranges	Limits
Confidence Level of AOU Cross-fix Ellipse	90 percent
Dynamic Status Board	1 master track / 20 slave tracks
Land Sites	100
Missile Systems/Track	10
Radar Systems/Track	10
Sonar Systems/Track	10
Weapon Systems/Track	10
Specific IFF Mode-2 Valued Tracks Can Be Archived	20
Track Archive Sequence of Steps	60 seconds
Track Groups	32
Tracks/Group	Limited only by disk storage
Track History Reports/Track	1,000
Track Symbol Label	26 characters

Table 8. Other Track Range Limits

Communications	Limits
Addressee (Channel Message Buffer Manager)	1,000 backlog messages
Alert Log	1,000 messages
Incoming Message Log	1,000 messages
Incoming Opnote Log	200 opnotes
Outgoing Message Log	1,000 messages
RAINFORM Messages	1,000 lines
Received Messages Displayed in Status Window	1,000 messages
Report Log	2,000 reports
Saved for Raw Messages	500 lines

Table 9. Communications Limits

Miscellaneous	Limits
Auto-Forwarding, Addresses	500
Broadcast, User-Set Cycle Rate	0-720 minutes
Broadcasts, Active	25
Characters Stored per Screen Name	50
Clipboard, Files Stored on	1,000
Engagement Scenarios	10
Grid Cells, Number of	24 or 48
IFF/DIs, Nicknames	100
Incoming Message Alert, Addresses	5
Incoming Message Alert, Originators	5
Net Address (DDN)	256
Satellite Charlie Elements	300
Satvul-Satellites per Category	300
Stored Screen, Briefing Slides	50
Stored Screens, Number of	50

Table 10. Miscellaneous Limits

Maps	Limits
Key Sites	1,000
Stored Map, Parameter Combinations	500
Stored Maps	20
Zoom Width, Greatest	21,600 NM
Zoom Width, Smallest	0.25 NM

Table 11. Map Limits

Overlays	Limits
Overlay, Items	100
Overlay, Points	256
Overlay, Polyline Points	256
Overlays, Number of	500

Table 12. Overlay Limits

This page intentionally left blank.

Appendix E - Allocating More Disk Space on an LVM Configured System

Follow the steps below to allocate more disk space on a logical volume manager (LVM) configured HP system using the HP-UX SAM.

STEP 1: **Log in as `root`**. Type `root` at the `Name` prompt and press [`RETURN`].

STEP 2: **Enter the `root` password**. Type the `root` password at the `Password` prompt and press [`RETURN`]. The CDE Front Panel appears at the bottom of the screen.

STEP 3: **Access the File Manager**. Double-click on the File Manager control on the CDE Front Panel to open the `File Manager` window. Reference Section 5, *Common Desktop Environment*, for more information about CDE.

STEP 4: **Select the `usr` folder**. Double-click on the `usr` folder, which is located in the `File Manager` window.

STEP 5: **Select the `sbin` folder**. Double-click on the `sbin` folder.

STEP 6: **Select the `sam` icon**. Double-click on the `sam` icon.

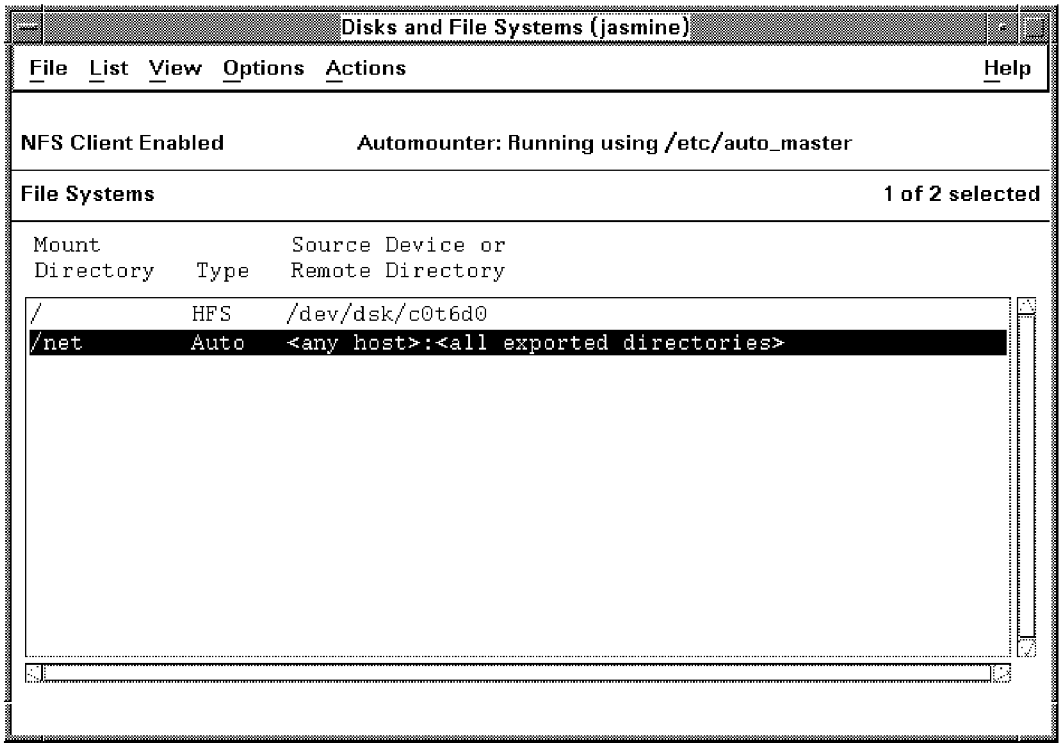
STEP 7: **Execute the SAM application**. The `Action: Execute` or `Action:Run` window appears. Click on the `OK` button without entering any options or arguments.

STEP 8: **Select the `Disks and File Systems` icon**. The `Welcome to SAM` window appears, followed by the `System Administration Manager` window. Inside the `System Administration Manager` window is the `SAM Areas` subwindow. Double-click on the `Disks and File Systems` icon.

STEP 9: **Select the `File Systems` icon**. The `SAM Areas:Disks and File Systems` subwindow appears. Double-click on the `File Systems` icon.

STEP 10: **Select the partition you want to modify**. The `Disks and File Systems` window appears (Figure 36). Click on the partition that you want to modify to highlight it.

STEP 11: **Choose to modify the partition**. Click on `Modify...` from the `Actions` pull-down menu.



NFS Client Enabled Automounter: Running using /etc/auto_master

File Systems 1 of 2 selected

```
Mount                Source Device or
Directory   Type     Remote Directory
/           HFS      /dev/dsk/c0t6d0
/net        Auto     <any host>:<all exported directories>
```

Figure 36. File Systems Window

STEP 12: **Unmount the partition**. The `Modify a Local File System`window appears. The partition to be modified must be unmounted before you can increase its size. Click on the `Now` toggle in the `When to Mount: (optional)`panel. The toggle will be deselected (gray). Click on the `OK` button.

WARNING: **Do NOT** unmount any partitions that are in use. This includes `/`, `/stand`, `/h`, and any NFS mount points.

STEP 13: **Confirm that you want to unmount the partition**. Click on the `Yes` button when a confirmation message similar to the following appears:

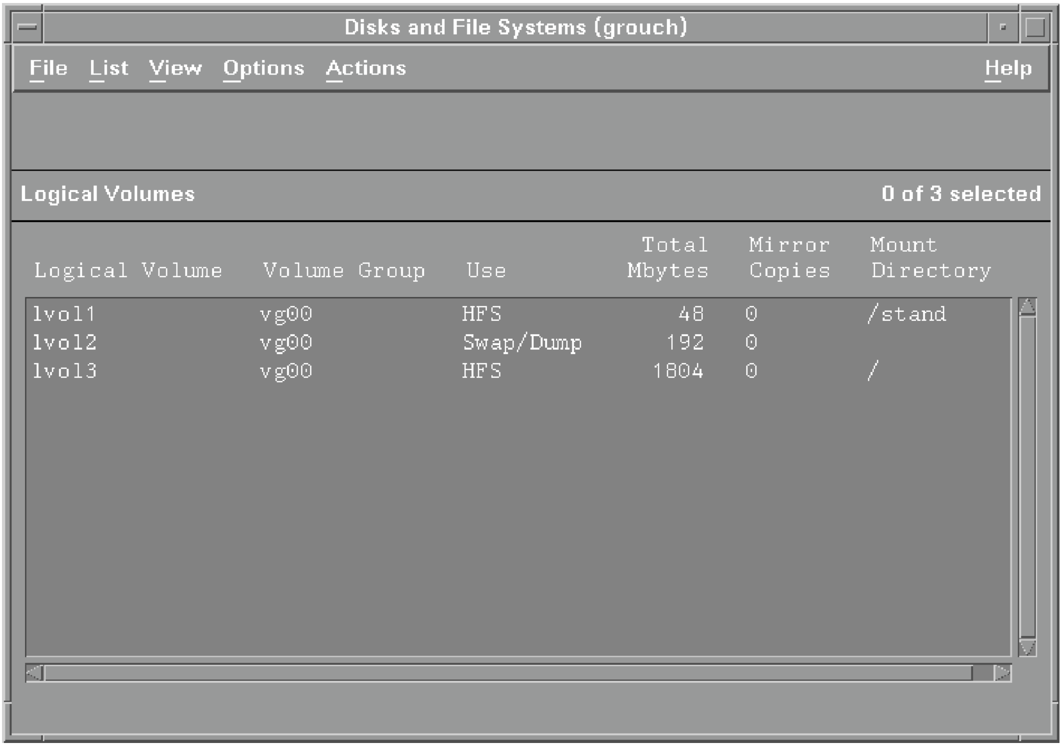
```
Removing the file system, [name of file system], means all
files in the file system will no longer be available.

Do you want to continue and remove the file system?
```

STEP 14: **Exit the `Disks and File Systems`window**. The `Disks and File Systems` window returns to the forefront. Click on `Exit` from the `File` pull-down menu.

STEP 15: **Choose to view logical volumes**. The `SAM Areas:Disks and File Systems` window appears. Double-click on the `Logical Volumes` icon.

STEP 16: **Select the volume that you want to increase**. The `Logical Volumes` subwindow appears (Figure 37). Click on the volume to be increased to highlight it. The sixth column, `Mount Directory`, shows the mount point.



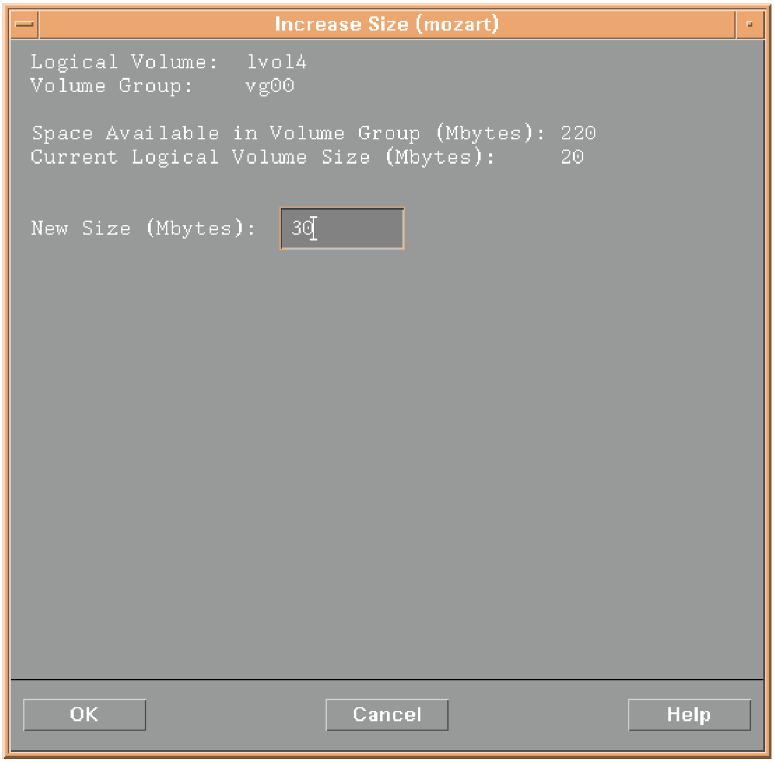
Logical Volumes 0 of 3 selected

Logical Volume	Volume Group	Use	Total Mbytes	Mirror Copies	Mount Directory
lvol1	vg00	HFS	48	0	/stand
lvol2	vg00	Swap/Dump	192	0	
lvol3	vg00	HFS	1804	0	/

Figure 37. Logical Volumes Window

STEP 17: **Choose to increase the volume**. Select `Increase Size...` from the `Actions` pull-down menu.

STEP 18: **Choose the new size of the volume**. The `Increase Size` window appears (Figure 38). The available space is shown in the `Space Available in Volume Group (Mbytes)` field. If any space is available in the volume group, you can increase the size of the volume. The current logical volume size is shown in the `Current Logical Volume Size (Mbytes)`field. Type the number in the `New Size (Mbytes)` field and click on the `OK` button.



```
Logical Volume:  lvol4
Volume Group:    vg00

Space Available in Volume Group (Mbytes): 220
Current Logical Volume Size (Mbytes):      20

New Size (Mbytes):  30
```

Figure 38. Increase Size Window

STEP 19: **Acknowledge a message that the size must be a multiple of 4 MB**. Click on the `OK` button if a message similar to the following appears:

```
When increasing the size of an existing logical volume, the
new size must be at least 4 Mbytes (the physical extent size
for this volume group) greater than the current size.
```

The size in the `Increase Size` window changes to a multiple of 4 Mbytes. Click on the `OK` button in the `Increase Size` window to continue.

STEP 20: **Check the partition size in the `Disks and File Systems` window**. If the modification was successful, the fourth column of the `Disks and File Systems` window, `Total Mbytes`, will display the increased size of the partition.

STEP 21: **Exit the `Disks and File Systems` window**. Select the `Exit` option from the `File` pull-down menu.

STEP 22: **Mount the partition whose size was increased**. From the `SAM Areas: Disks and File Systems` window, double-click on the `File Systems` icon.

STEP 23: **Select the modified partition**. The `File Systems` window appears. Click on the partition that was unmounted and then modified to highlight it.

STEP 24: **Choose to modify the partition**. Click on `Modify...` from the `Actions` pull-down menu.

STEP 25: **Mount the partition**. Click on the `Now` toggle in the `When to Mount: (Optional)` column. The toggle will be selected (white). Click on the `OK` button.

STEP 26: **Exit the `Disks and File Systems` window**. Click on the `Exit` option from the `File` pull-down menu to exit the `Disks and File Systems` window.

STEP 27: **Exit SAM**. Click on the `Exit SAM` option from the `File` menu to exit SAM.

This page intentionally left blank.